Monthly Security Tips Newsletter
September 2008

CISO Tips

Remember to protect your home computer from access to unsafe and undesirable sites.
Try Blue Coat's™ free home offering at http://www1.k9webprotection.com/;

To view State security policies, please visit: http://isd.alabama.gov/policies/policies.aspx?sm=c_a;
Please see the new look and visit the Policies/Security & Security/Compliance links.

Remember to continue to contact the ISD Helpdesk with all Security questions/incidents @ help.desk@isd.alabama.gov
*ALERT: please see "**Revised!**" security documents: Policy 640-03, Standards 670-05S1, 680-03S1
*ALERT: please see "**NEW!**" security documents: Guideline 660-02G6

Personal Privacy – How to Protect Your Information

As we continue to conduct more business online, such as banking, shopping and other activities, our personal information (such as name, credit card account, address, etc) is increasingly utilized. Personal information has become a frequent target for data thieves and the volume of breaches involving personal information continues to grow. According to the Privacy Rights Clearinghouse, there have been more than 240 million records containing sensitive personal information involved in security breaches to-date nationally.

What Personal Information is Collected?
Many types of organizations are interested in obtaining and using your personal information, and it's important to know what information is being collected, by whom and how it will be used.

Websites track web users as they navigate cyberspace. Data may be collected about you as a result of many of your routine activities including:

- When you make purchases and pay bills with credit cards, you leave a data trail consisting of purchase amount, purchase type, date, and time.
- When you pay by check, data such as phone number, home address, driver's license number, etc. may often be requested to verify your identity.
- When you use supermarket discount cards, the store is able to create a comprehensive database of everything you have purchased.
- When you surf the web, you leave a significant data trail such as your name, email address, Internet address of your computer, the name of your computer, the last time you visited that particular site, the type of browser and operating system you are using.
- When you sign up for a subscription or service (for a magazine, book or music club, professional association, warranty card, etc.) or give money to charities your personal information is often collected and stored.

Protecting Your Personal Information
The following tips should be used to help you manage your personal information wisely, to help minimize its misuse, and to lessen the risk of your personal information being compromised:

- Most legitimate websites include a privacy statement. This is usually a link at the bottom of the home page and details the type of personally identifiable information the site collects about its visitors, how the information is used—including with whom it may be shared— and

how users can control the information that is gathered. Be sure to read the privacy statement on websites you are visiting **prior** to providing any personal information, to understand that entity's policy regarding protection of data.

- When shopping online, guard the security of your transactions by ensuring the transaction is submitted securely. When submitting your purchase information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.
- Periodically check your Internet browser settings (e.g. Security and Privacy) to ensure that the settings are adequate for your level and type of Internet activity.
- If you are not already using anti-spyware or adware protection software, start now. This software is designed to protect against spyware or malware designed to extract private information from your computer without your knowledge. Make sure you keep the anti-spyware or adware protection programs updated.
- Be sure to have a firewall installed and enabled on your computer.
- If you store private data on your laptop or other portable electronic devices (e.g. USB), use encryption software to protect your private data in the event the device is lost or stolen.
- Use strong passwords on all your accounts, such as a minimum of eight characters and a mix of special symbols, letters and numbers.
- To protect against identity theft, always question someone who is asking you to reveal any personably identifiable information. Find out how it will be used and whether it will be shared with others.
- Keep items with personal information in a safe place. When you discard receipts, copies of credit applications, insurance forms, health records, bank statements, or other personal documents, tear or shred them.
- Order a copy of your free annual credit report. Make sure it's accurate and includes only those activities you've authorized.

References:
To learn more about protecting your privacy, please visit the following sites:

- Identity Theft: www.ftc.gov/bcp/menus/consumer/data/idt.shtm
- Consumer Action: www.consumer-action.org
- Electronic Privacy Information Center: www.epic.org
- Privacy Rights Clearinghouse: www.privacyrights.org
- World Privacy Forum: www.worldprivacyforum.org
- Free Annual Credit Report: www.annualcreditreport.com [review policies for costs]
- US-CERT Tips for Strong Passwords: www.uscert.gov/cas/tips/ST04-002.html

Resources:
For previous issues of the Monthly Cyber Security Tips Newsletters visit:
www.msisac.org/awareness/news/

MS-ISAC

http://www.msisac.org